Finding a Needle in a PCAP

Flocon 2015

Emily Sarneso

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **27 JAN 2015**	2. REPORT TYPE **N/A**	3. DATES COVERED
4. TITLE AND SUBTITLE **Finding a Needle in a PCAP**		5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Sarneso /Emily**		5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**27**	

This material is based upon work supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University of its Software Engineering Institute.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0001893

Goal

Describe a full packet capture solution that can quickly and efficiently produce requested information.

Show analysis capabilities of YAF, super_mediator, and SiLK.

Demonstrate PCAP features in YAF.

PCAP Challenges

Volume (4Gbps):

- 1 Hour: 1.7TB
- 1 Day: 40.8TB
- 1 Week: 285.6TB
- 1 Month: 1.1PB

Data Stored on Sensors

- Separate from analysis

Indexing:

- Timestamp Files
- BPF Filters
- GUI tools
- Splunk

jolyon.co.uk

YAF PCAP Features

Rolling PCAP dump

- Rotates files using time or size.
- Creates meta file with flows contained in each PCAP file.

Index a PCAP File

- Uses flow key hash and start time.

PCAP per flow

- Creates a PCAP file for each flow.
- Use with BPF filters.

Gh0st Rat Investigation

Gh0st

Chinese remote access Trojan

Free source code

Easy to modify

Distinctive Network Signature

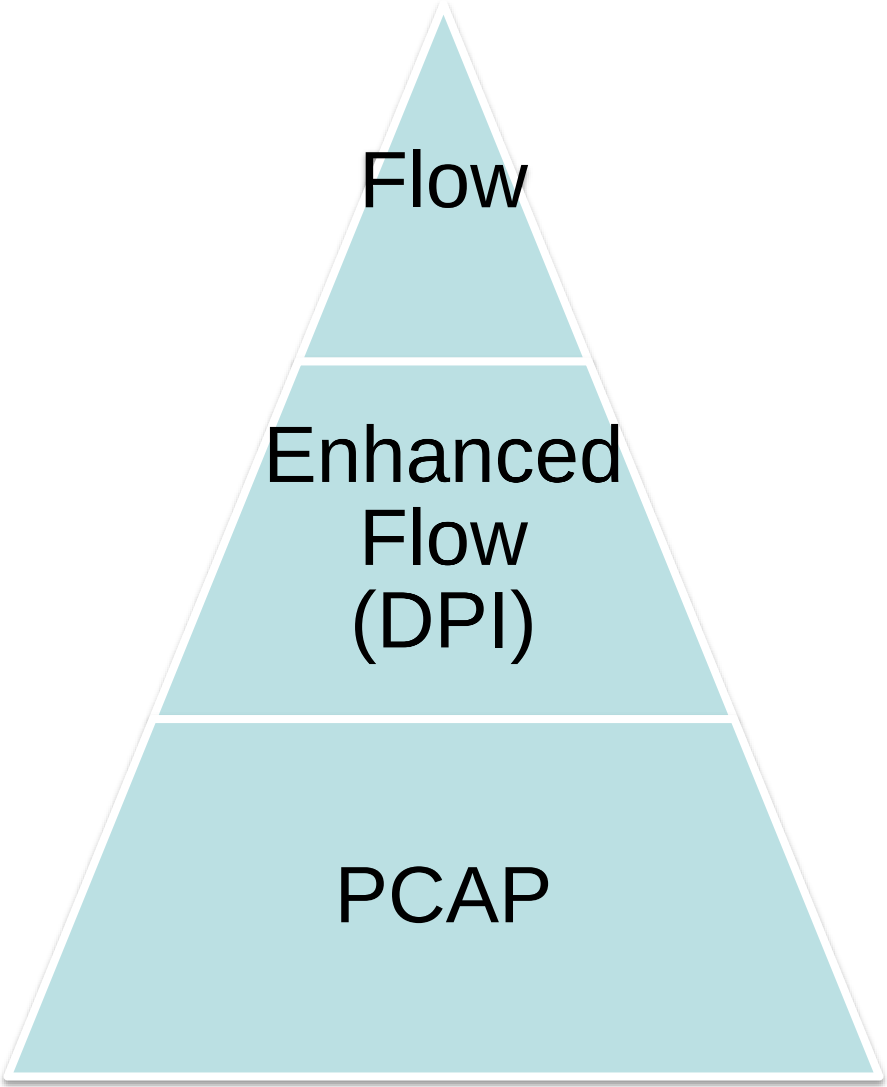
Signature	Compressed Length	Uncompressed Length	ZLIBHDR 0x789C	Data
Usually 5 BYTES	4 BYTES	4 BYTES	2 BYTES	

Method

29,000 (15G) PCAP samples

Use YAF to index and produce flow, DPI

YAF Signatures

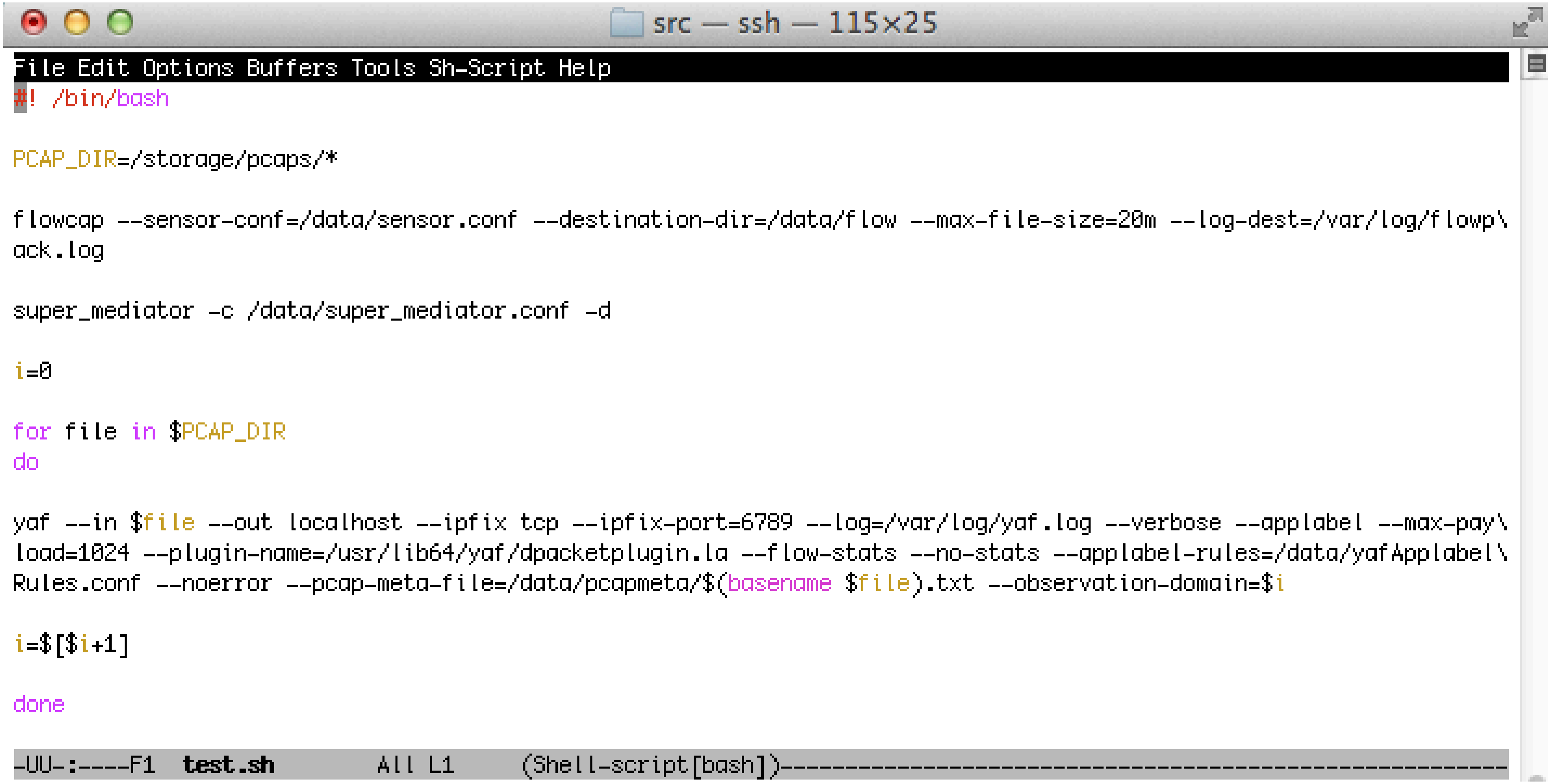


Flow

Enhanced Flow (DPI)

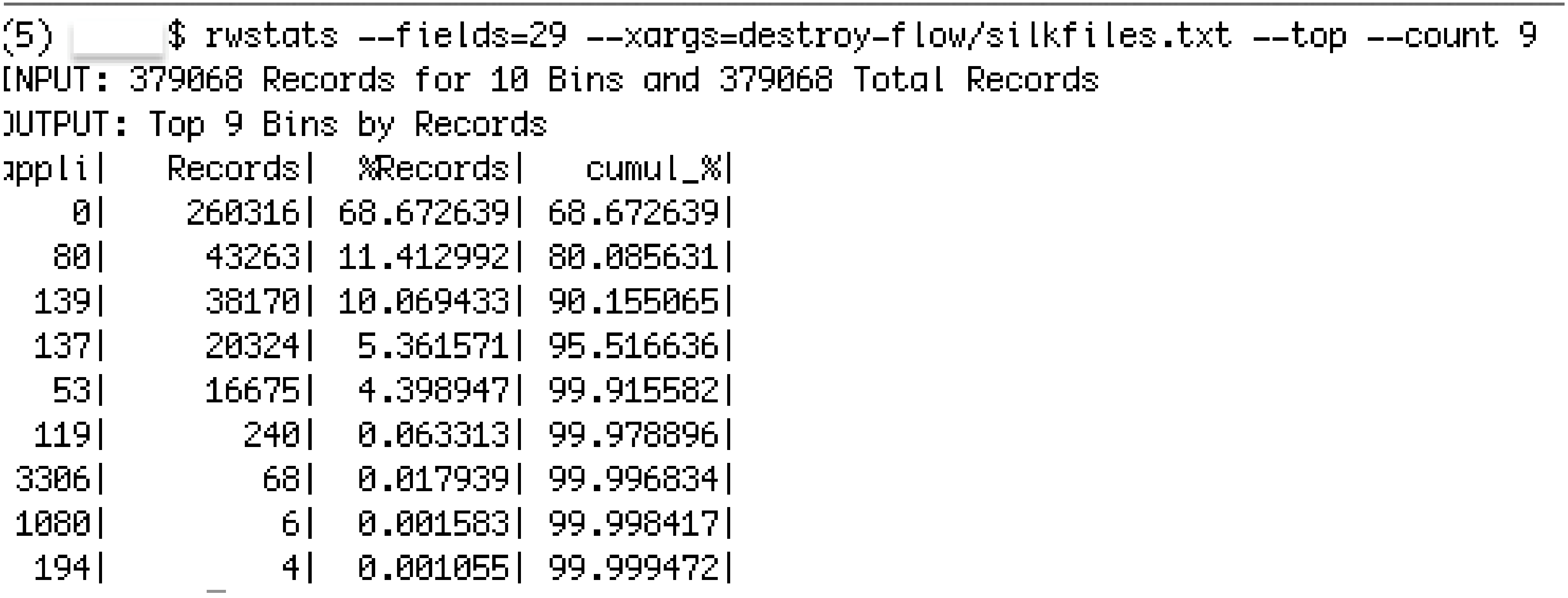
PCAP

Tool setup



```
#! /bin/bash

PCAP_DIR=/storage/pcaps/*

flowcap --sensor-conf=/data/sensor.conf --destination-dir=/data/flow --max-file-size=20m --log-dest=/var/log/flowp\
ack.log

super_mediator -c /data/super_mediator.conf -d

i=0

for file in $PCAP_DIR
do

yaf --in $file --out localhost --ipfix tcp --ipfix-port=6789 --log=/var/log/yaf.log --verbose --applabel --max-pay\
load=1024 --plugin-name=/usr/lib64/yaf/dpacketplugin.la --flow-stats --no-stats --applabel-rules=/data/yafApplabel\
Rules.conf --noerror --pcap-meta-file=/data/pcapmeta/$(basename $file).txt --observation-domain=$i

i=$[$i+1]

done

-UU-:----F1  test.sh        All L1     (Shell-script[bash])------------------------------------------------
```

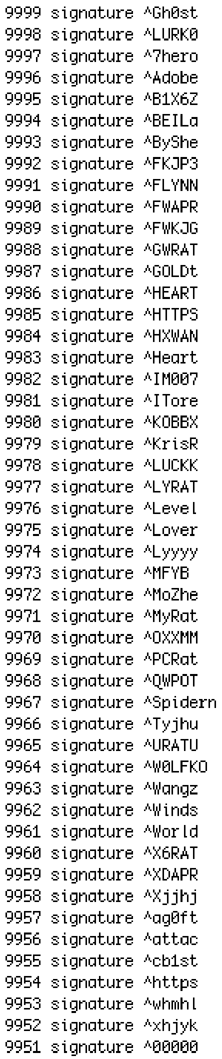
Initial Results



```
(5) [redacted]$ rwstats --fields=29 --xargs=destroy-flow/silkfiles.txt --top --count 9
INPUT: 379068 Records for 10 Bins and 379068 Total Records
OUTPUT: Top 9 Bins by Records
appli|   Records|  %Records|   cumul_%|
    0|    260316| 68.672639| 68.672639|
   80|     43263| 11.412992| 80.085631|
  139|     38170| 10.069433| 90.155065|
  137|     20324|  5.361571| 95.516636|
   53|     16675|  4.398947| 99.915582|
  119|       240|  0.063313| 99.978896|
 3306|        68|  0.017939| 99.996834|
 1080|         6|  0.001583| 99.998417|
  194|         4|  0.001055| 99.999472|
```

YAF Signatures

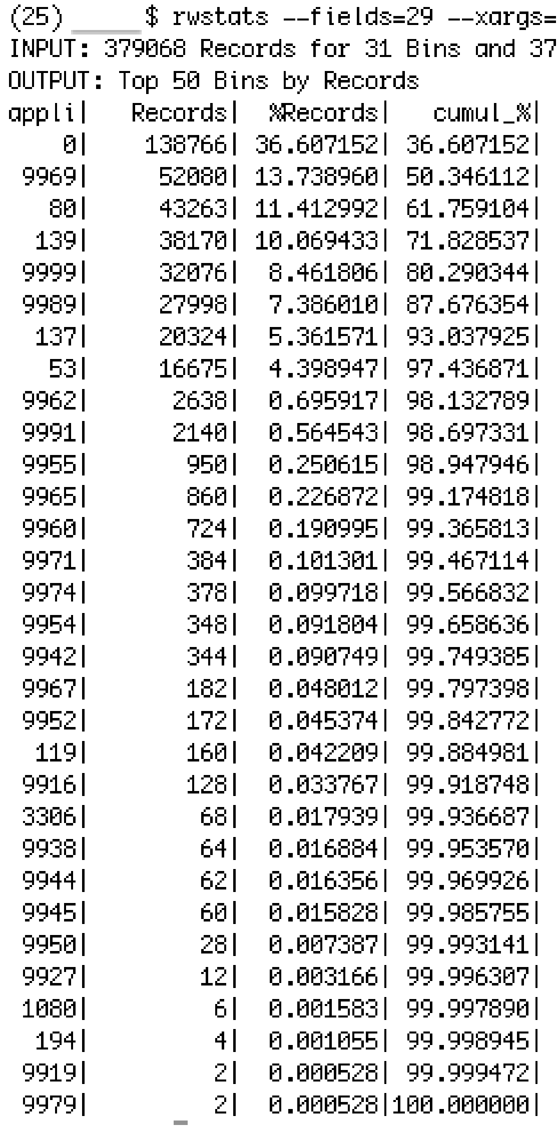
Norman ASA 2012 Report identifies 85 Gh0st variants



```
9999 signature ^Gh0st
9998 signature ^LURK0
9997 signature ^7hero
9996 signature ^Adobe
9995 signature ^B1X6Z
9994 signature ^BEILa
9993 signature ^ByShe
9992 signature ^FKJP3
9991 signature ^FLYNN
9990 signature ^FWAPR
9989 signature ^FWKJG
9988 signature ^GWRAT
9987 signature ^GOLDt
9986 signature ^HEART
9985 signature ^HTTPS
9984 signature ^HXWAN
9983 signature ^Heart
9982 signature ^IM007
9981 signature ^ITore
9980 signature ^KOBBX
9979 signature ^KrisR
9978 signature ^LUCKK
9977 signature ^LYRAT
9976 signature ^Level
9975 signature ^Lover
9974 signature ^Lyyyy
9973 signature ^MFYB
9972 signature ^MoZhe
9971 signature ^MyRat
9970 signature ^OXXMM
9969 signature ^PCRat
9968 signature ^QWPOT
9967 signature ^Spidern
9966 signature ^Tyjhu
9965 signature ^URATU
9964 signature ^W0LFKO
9963 signature ^Wangz
9962 signature ^Winds
9961 signature ^World
9960 signature ^X6RAT
9959 signature ^XDAPR
9958 signature ^Xjjhj
9957 signature ^ag0ft
9956 signature ^attac
9955 signature ^cb1st
9954 signature ^https
9953 signature ^whmhl
9952 signature ^xhjyk
9951 signature ^00000
```

download01.**norman**.no/documents/Themanyfacesof**Gh0st**Rat.pdf

Results with YAF Signatures



```
(25)      $ rwstats --fields=29 --xargs=destroy-flow/silkfiles.txt --top --count=50
INPUT: 379068 Records for 31 Bins and 379068 Total Records
OUTPUT: Top 50 Bins by Records
appli|   Records|  %Records|   cumul_%|
    0|    138766| 36.607152| 36.607152|
 9969|     52080| 13.738960| 50.346112|
   80|     43263| 11.412992| 61.759104|
  139|     38170| 10.069433| 71.828537|
 9999|     32076|  8.461806| 80.290344|
 9989|     27998|  7.386010| 87.676354|
  137|     20324|  5.361571| 93.037925|
   53|     16675|  4.398947| 97.436871|
 9962|      2638|  0.695917| 98.132789|
 9991|      2140|  0.564543| 98.697331|
 9955|       950|  0.250615| 98.947946|
 9965|       860|  0.226872| 99.174818|
 9960|       724|  0.190995| 99.365813|
 9971|       384|  0.101301| 99.467114|
 9974|       378|  0.099718| 99.566832|
 9954|       348|  0.091804| 99.658636|
 9942|       344|  0.090749| 99.749385|
 9967|       182|  0.048012| 99.797398|
 9952|       172|  0.045374| 99.842772|
  119|       160|  0.042209| 99.884981|
 9916|       128|  0.033767| 99.918748|
 3306|        68|  0.017939| 99.936687|
 9938|        64|  0.016884| 99.953570|
 9944|        62|  0.016356| 99.969926|
 9945|        60|  0.015828| 99.985755|
 9950|        28|  0.007387| 99.993141|
 9927|        12|  0.003166| 99.996307|
 1080|         6|  0.001583| 99.997890|
  194|         4|  0.001055| 99.998945|
 9919|         2|  0.000528| 99.999472|
 9979|         2|  0.000528|100.000000|
```

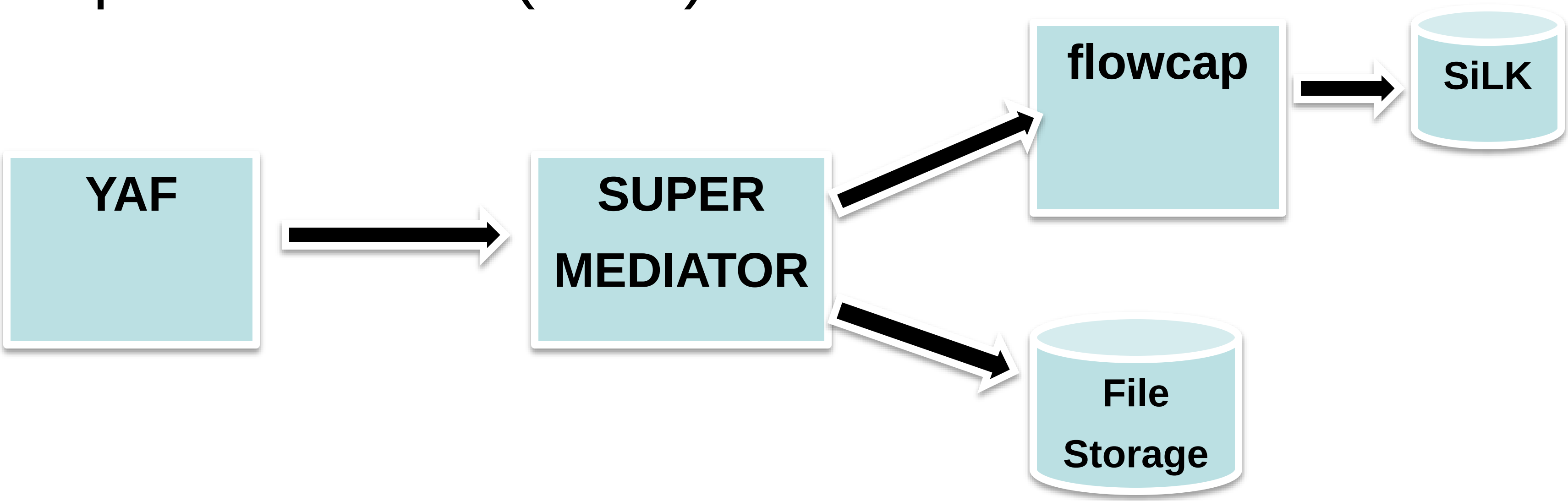
Super_mediator

A very configurable IPFIX mediator

Collects every IPFIX information element YAF can export

Multiple exporters

Multiple collectors (v.1.0)



Super_mediator configuration

Listing application label first allowed for quick binning by variant.

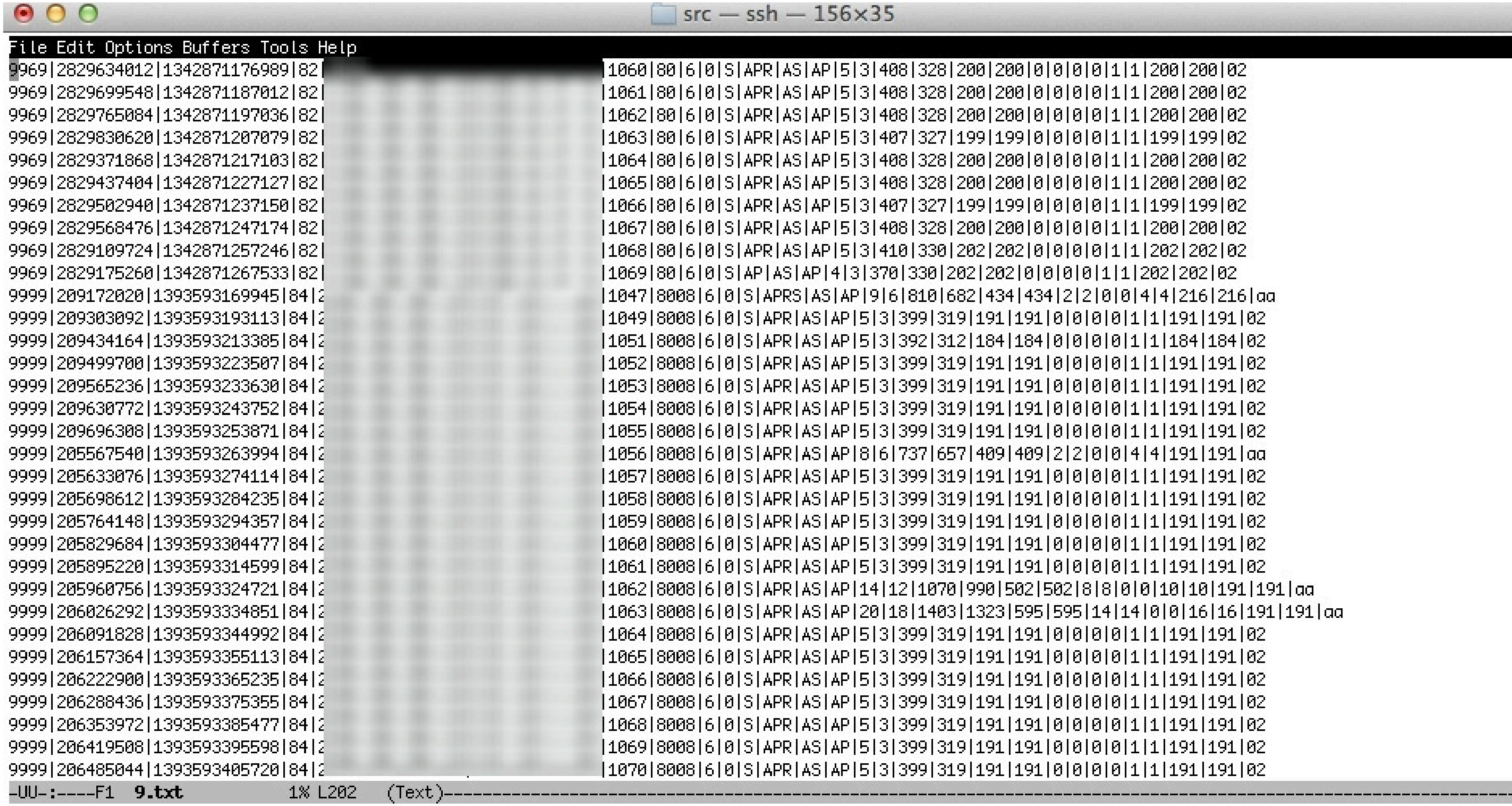
Super_mediator Results:

- 227,833 Total Bi-flows
- 60,816 Bi-flows Gh0st
- 86,053 Unidentified

Application
Hash
Stimems
Domain
Sip
Dip
Sport
Dport
Protocol
vlanint
Iflags
Uflags
Riflags
Ruflags
Pkts,
Rpkts

Bytes
Rbytes
Databytes
Rdatabytes
Smallpkts
Rsmallpkts
Largepkts
Rlargepkts
Nonemptypkts
Rnonemptypkts
Maxsize
Rmaxsize
Firsteight

Finding a Pattern



```
9969|2829634012|1342871176989|82|[redacted]|1060|80|6|0|S|APR|AS|AP|5|3|408|328|200|200|0|0|0|0|1|1|200|200|02
9969|2829699548|1342871187012|82|[redacted]|1061|80|6|0|S|APR|AS|AP|5|3|408|328|200|200|0|0|0|0|1|1|200|200|02
9969|2829765084|1342871197036|82|[redacted]|1062|80|6|0|S|APR|AS|AP|5|3|408|328|200|200|0|0|0|0|1|1|200|200|02
9969|2829830620|1342871207079|82|[redacted]|1063|80|6|0|S|APR|AS|AP|5|3|407|327|199|199|0|0|0|0|1|1|199|199|02
9969|2829371868|1342871217103|82|[redacted]|1064|80|6|0|S|APR|AS|AP|5|3|408|328|200|200|0|0|0|0|1|1|200|200|02
9969|2829437404|1342871227127|82|[redacted]|1065|80|6|0|S|APR|AS|AP|5|3|408|328|200|200|0|0|0|0|1|1|200|200|02
9969|2829502940|1342871237150|82|[redacted]|1066|80|6|0|S|APR|AS|AP|5|3|407|327|199|199|0|0|0|0|1|1|199|199|02
9969|2829568476|1342871247174|82|[redacted]|1067|80|6|0|S|APR|AS|AP|5|3|408|328|200|200|0|0|0|0|1|1|200|200|02
9969|2829109724|1342871257246|82|[redacted]|1068|80|6|0|S|APR|AS|AP|5|3|410|330|202|202|0|0|0|0|1|1|202|202|02
9969|2829175260|1342871267533|82|[redacted]|1069|80|6|0|S|AP|AS|AP|4|3|370|330|202|202|0|0|0|0|1|1|202|202|02
9999|209172020|1393593169945|84|[redacted]|1047|8008|6|0|S|APRS|AS|AP|9|6|810|682|434|434|2|2|0|0|4|4|216|216|aa
9999|209303092|1393593193113|84|[redacted]|1049|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
9999|209434164|1393593213385|84|[redacted]|1051|8008|6|0|S|APR|AS|AP|5|3|392|312|184|184|0|0|0|0|1|1|184|184|02
9999|209499700|1393593223507|84|[redacted]|1052|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
9999|209565236|1393593233630|84|[redacted]|1053|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
9999|209630772|1393593243752|84|[redacted]|1054|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
9999|209696308|1393593253871|84|[redacted]|1055|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
9999|205567540|1393593263994|84|[redacted]|1056|8008|6|0|S|APR|AS|AP|8|6|737|657|409|409|2|2|0|0|4|4|191|191|aa
9999|205633076|1393593274114|84|[redacted]|1057|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
9999|205698612|1393593284235|84|[redacted]|1058|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
9999|205764148|1393593294357|84|[redacted]|1059|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
9999|205829684|1393593304477|84|[redacted]|1060|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
9999|205895220|1393593314599|84|[redacted]|1061|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
9999|205960756|1393593324721|84|[redacted]|1062|8008|6|0|S|APR|AS|AP|14|12|1070|990|502|502|8|8|0|0|10|10|191|191|aa
9999|206026292|1393593334851|84|[redacted]|1063|8008|6|0|S|APR|AS|AP|20|18|1403|1323|595|595|14|14|0|0|16|16|191|191|aa
9999|206091828|1393593344992|84|[redacted]|1064|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
9999|206157364|1393593355113|84|[redacted]|1065|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
9999|206222900|1393593365235|84|[redacted]|1066|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
9999|206288436|1393593375355|84|[redacted]|1067|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
9999|206353972|1393593385477|84|[redacted]|1068|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
9999|206419508|1393593395598|84|[redacted]|1069|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
9999|206485044|1393593405720|84|[redacted]|1070|8008|6|0|S|APR|AS|AP|5|3|399|319|191|191|0|0|0|0|1|1|191|191|02
-UU-:----F1  9.txt          1% L202   (Text)--------------------------------------------------------------------------------------------
```

Analysis Part 1

Remove unwanted flows from unidentified flows:

- Remove flows with source/destination port 138,139.
- Remove flows with initialTCPFlags = ‘R’
- Remove flows with dataByteCount = 0

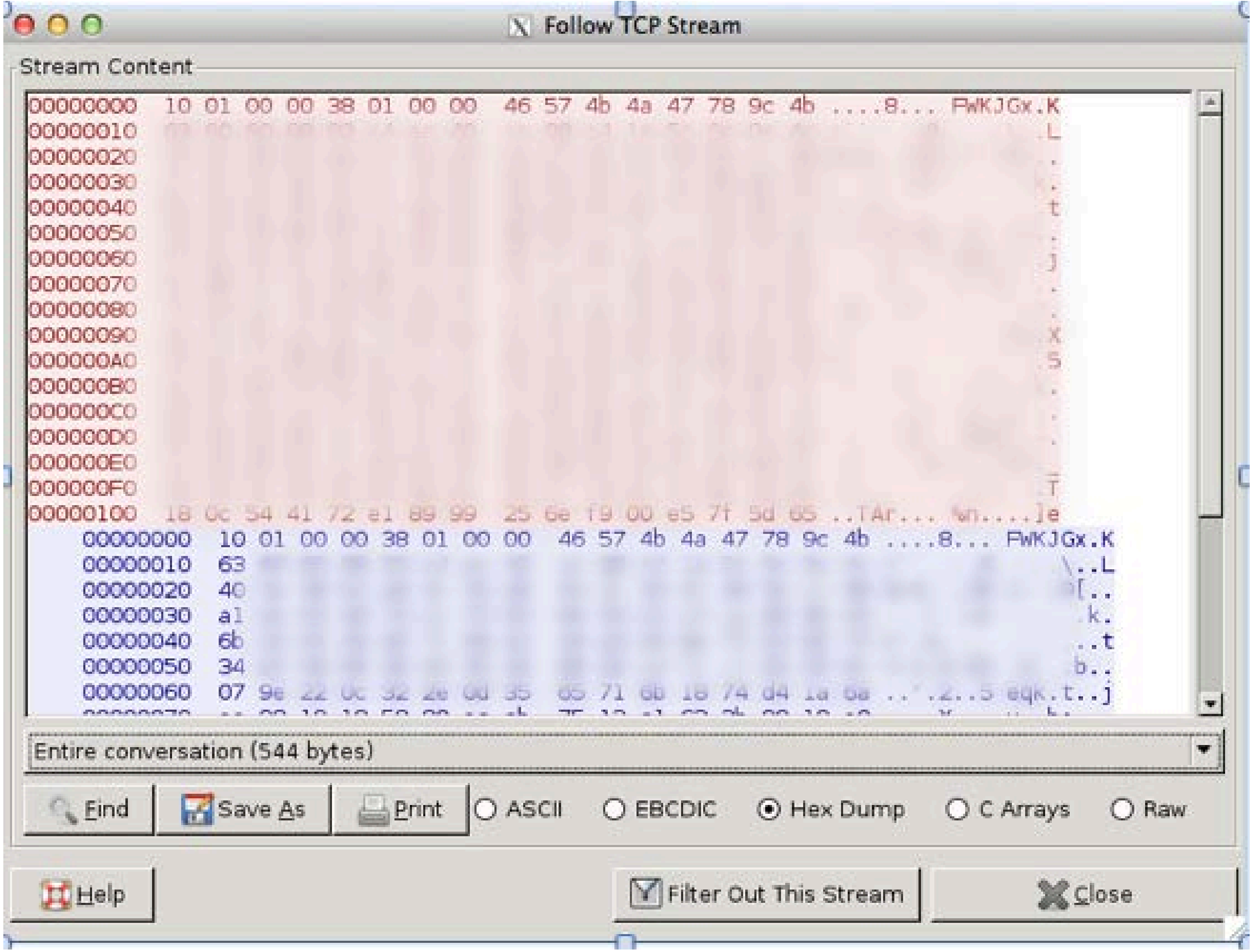
Find flows with pattern:

- No more than 1 small packet (forward), 0 reverse
- Non-empty packets = 1 or 2 (forward), 1 reverse
- maxPacketSize = reverseMaxPacketSize
- firstEightPacketDirection = 0x02

Results:

- 44,468 bi-flows removed
- 37,500 bi-flows with pattern
- 4,085 bi-flows did not follow pattern

Finding Gh0st Variants and Signatures

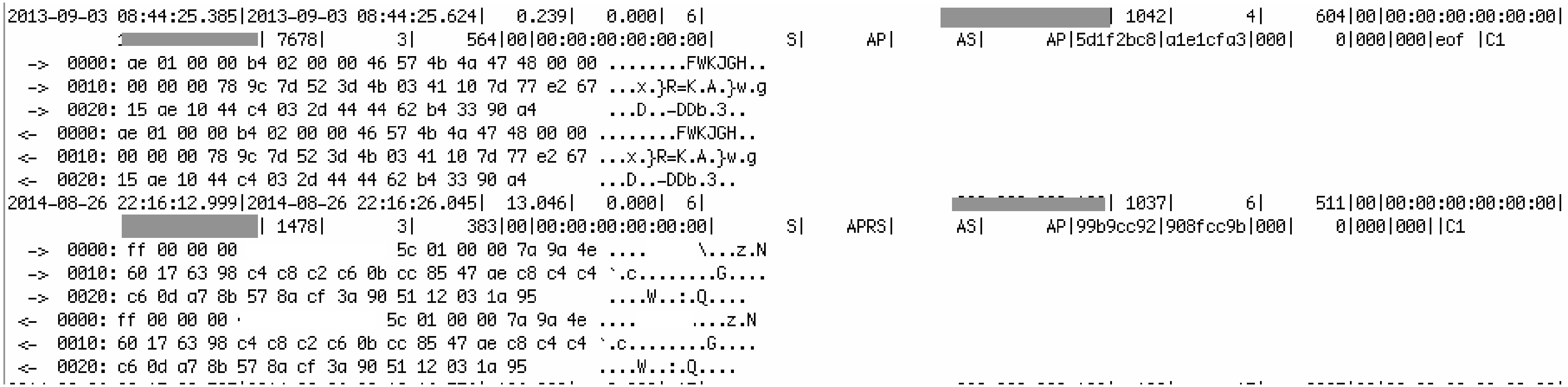


```
00000000  10 01 00 00 38 01 00 00  46 57 4b 4a 47 78 9c 4b ....8... FWKJGx.K
00000010  [redacted] .L
00000020  [redacted] .
00000030  [redacted] .
00000040  [redacted] t
00000050  [redacted] .
00000060  [redacted] j
00000070  [redacted] .
00000080  [redacted] .
00000090  [redacted] X
000000A0  [redacted] 5
000000B0  [redacted] .
000000C0  [redacted] .
000000D0  [redacted] .
000000E0  [redacted] .
000000F0  [redacted] T
00000100  18 0c 54 41 72 e1 89 99  25 6e f9 00 e5 7f 5d 65 ..TAr... %n....]e
    00000000  10 01 00 00 38 01 00 00  46 57 4b 4a 47 78 9c 4b ....8... FWKJGx.K
    00000010  63 [redacted] \..L
    00000020  40 [redacted] [..
    00000030  a1 [redacted] k.
    00000040  6b [redacted] ..t
    00000050  34 [redacted] b..
    00000060  07 9e 22 0c 32 2e 0d 35  65 71 6b 18 74 d4 1a 6a ..".2..5 eqk.t..j
```

Entire conversation (544 bytes)

Analysis Part 2

Run unidentified PCAP files through YAF again and export first 100 bytes of payload



```
2013-09-03 08:44:25.385|2013-09-03 08:44:25.624|   0.239|   0.000|  6|                    [redacted]| 1042|       4|     604|00|00:00:00:00:00:00|
          [redacted]| 7678|       3|     564|00|00:00:00:00:00:00|       S|      AP|      AS|      AP|5d1f2bc8|a1e1cfa3|000|    0|000|000|eof |C1
  ->  0000: ae 01 00 00 b4 02 00 00 46 57 4b 4a 47 48 00 00 ........FWKJGH..
  ->  0010: 00 00 00 78 9c 7d 52 3d 4b 03 41 10 7d 77 e2 67 ...x.}R=K.A.}w.g
  ->  0020: 15 ae 10 44 c4 03 2d 44 44 62 b4 33 90 a4       ...D..-DDb.3..
 <-  0000: ae 01 00 00 b4 02 00 00 46 57 4b 4a 47 48 00 00 ........FWKJGH..
 <-  0010: 00 00 00 78 9c 7d 52 3d 4b 03 41 10 7d 77 e2 67 ...x.}R=K.A.}w.g
 <-  0020: 15 ae 10 44 c4 03 2d 44 44 62 b4 33 90 a4       ...D..-DDb.3..
2014-08-26 22:16:12.999|2014-08-26 22:16:26.045|  13.046|   0.000|  6|                    [redacted]| 1037|       6|     511|00|00:00:00:00:00:00|
          [redacted]| 1478|       3|     383|00|00:00:00:00:00:00|       S|    APRS|      AS|      AP|99b9cc92|908fcc9b|000|    0|000|000||C1
  ->  0000: ff 00 00 00                5c 01 00 00 7a 9a 4e ....     \...z.N
  ->  0010: 60 17 63 98 c4 c8 c2 c6 0b cc 85 47 ae c8 c4 c4 `.c........G....
  ->  0020: c6 0d a7 8b 57 8a cf 3a 90 51 12 03 1a 95       ....W..:.Q....
 <-  0000: ff 00 00 00                5c 01 00 00 7a 9a 4e ....     ....z.N
 <-  0010: 60 17 63 98 c4 c8 c2 c6 0b cc 85 47 ae c8 c4 c4 `.c........G....
 <-  0020: c6 0d a7 8b 57 8a cf 3a 90 51 12 03 1a 95       ....W..:.Q....
```

Results

Identified several signature variants of Gh0st

Found 55 new Gh0st variants

Created YAF Application Label for Gh0st

- Correctly identifies 97% of Gh0st traffic.

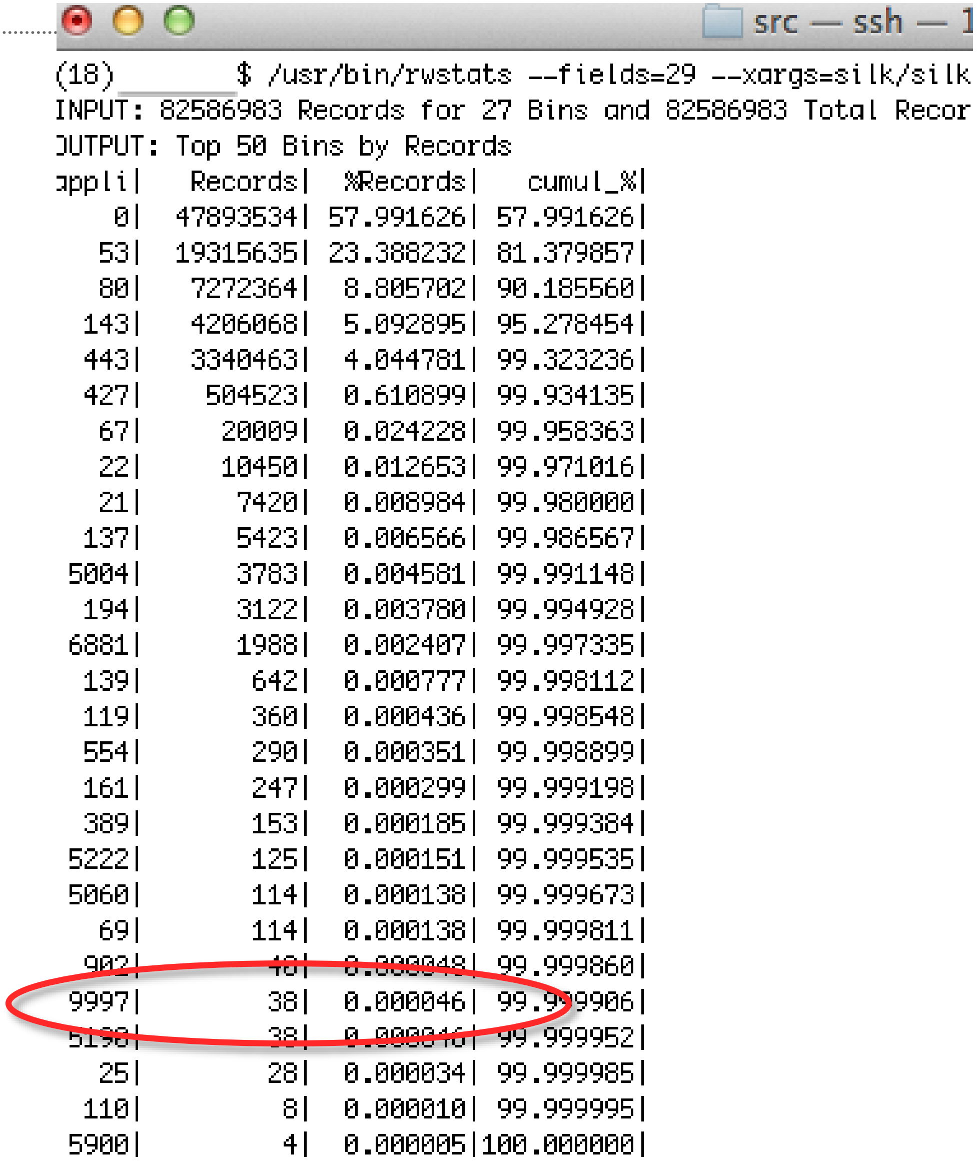
Searching for Gh0st in DEFCON CTF PCAP

DEFCON CTF PCAP Data

Goal: Test new Gh0st application label

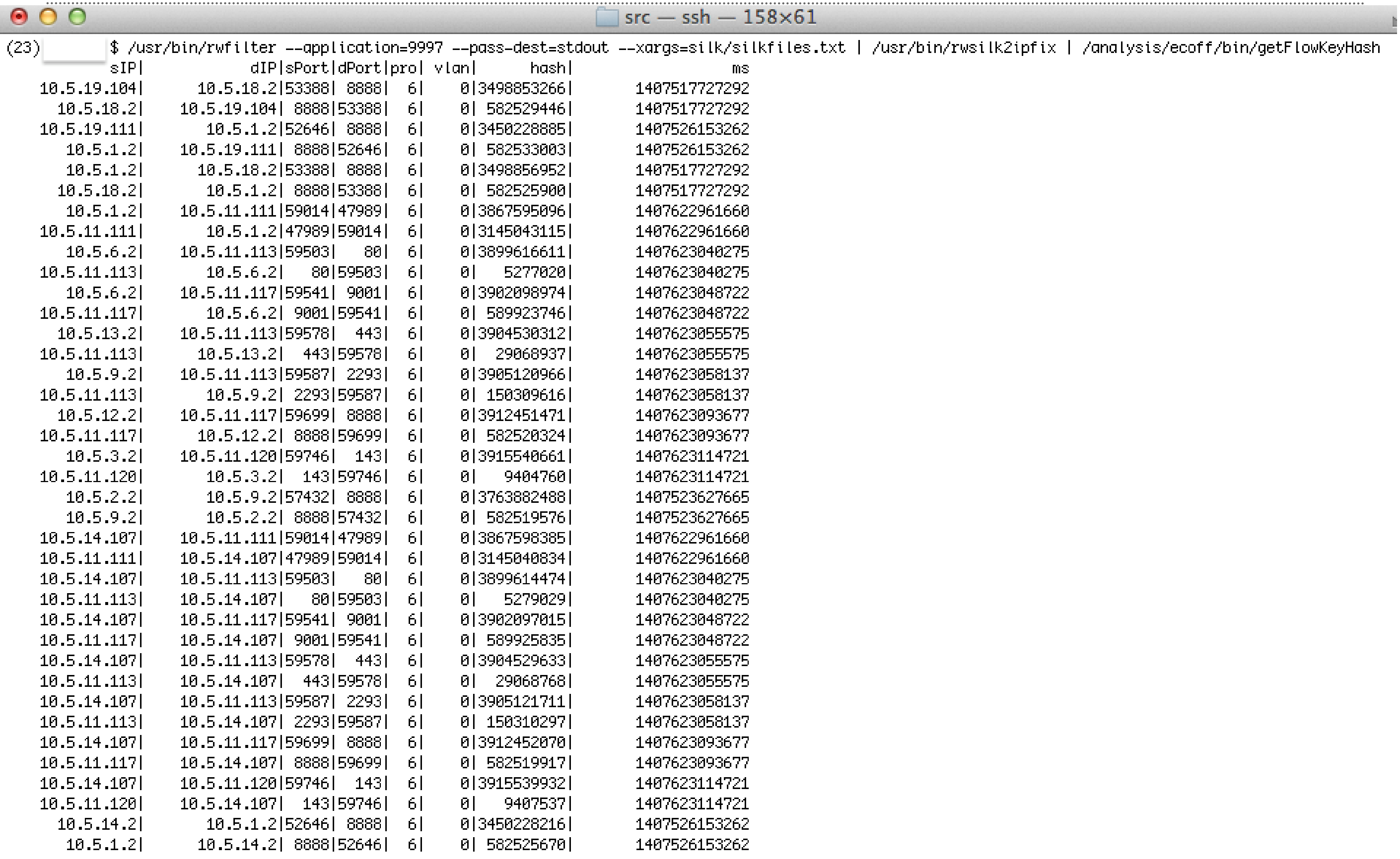
Defcon CTF PCAP Data

- 409 GB
- Separated by team and day



```
(18)          $ /usr/bin/rwstats --fields=29 --xargs=silk/silk
INPUT: 82586983 Records for 27 Bins and 82586983 Total Recor
OUTPUT: Top 50 Bins by Records
appli|   Records|  %Records|   cumul_%|
    0|  47893534| 57.991626| 57.991626|
   53|  19315635| 23.388232| 81.379857|
   80|   7272364|  8.805702| 90.185560|
  143|   4206068|  5.092895| 95.278454|
  443|   3340463|  4.044781| 99.323236|
  427|    504523|  0.610899| 99.934135|
   67|     20009|  0.024228| 99.958363|
   22|     10450|  0.012653| 99.971016|
   21|      7420|  0.008984| 99.980000|
  137|      5423|  0.006566| 99.986567|
 5004|      3783|  0.004581| 99.991148|
  194|      3122|  0.003780| 99.994928|
 6881|      1988|  0.002407| 99.997335|
  139|       642|  0.000777| 99.998112|
  119|       360|  0.000436| 99.998548|
  554|       290|  0.000351| 99.998899|
  161|       247|  0.000299| 99.999198|
  389|       153|  0.000185| 99.999384|
 5222|       125|  0.000151| 99.999535|
 5060|       114|  0.000138| 99.999673|
   69|       114|  0.000138| 99.999811|
  902|        40|  0.000048| 99.999860|
 9997|        38|  0.000046| 99.999906|
 5198|        38|  0.000046| 99.999952|
   25|        28|  0.000034| 99.999985|
  110|         8|  0.000010| 99.999995|
 5900|         4|  0.000005|100.000000|
```

Investigating “Gh0st” in DEFCON



```
(23) [redacted] $ /usr/bin/rwfilter --application=9997 --pass-dest=stdout --xargs=silk/silkfiles.txt | /usr/bin/rwsilk2ipfix | /analysis/ecoff/bin/getFlowKeyHash
            sIP|            dIP|sPort|dPort|pro| vlan|      hash|                  ms
    10.5.19.104|      10.5.18.2|53388| 8888|  6|    0|3498853266|       1407517727292
      10.5.18.2|    10.5.19.104| 8888|53388|  6|    0| 582529446|       1407517727292
    10.5.19.111|       10.5.1.2|52646| 8888|  6|    0|3450228885|       1407526153262
       10.5.1.2|    10.5.19.111| 8888|52646|  6|    0| 582533003|       1407526153262
       10.5.1.2|      10.5.18.2|53388| 8888|  6|    0|3498856952|       1407517727292
      10.5.18.2|       10.5.1.2| 8888|53388|  6|    0| 582525900|       1407517727292
       10.5.1.2|    10.5.11.111|59014|47989|  6|    0|3867595096|       1407622961660
    10.5.11.111|       10.5.1.2|47989|59014|  6|    0|3145043115|       1407622961660
       10.5.6.2|    10.5.11.113|59503|   80|  6|    0|3899616611|       1407623040275
    10.5.11.113|       10.5.6.2|   80|59503|  6|    0|   5277020|       1407623040275
       10.5.6.2|    10.5.11.117|59541| 9001|  6|    0|3902098974|       1407623048722
    10.5.11.117|       10.5.6.2| 9001|59541|  6|    0| 589923746|       1407623048722
      10.5.13.2|    10.5.11.113|59578|  443|  6|    0|3904530312|       1407623055575
    10.5.11.113|      10.5.13.2|  443|59578|  6|    0|  29068937|       1407623055575
       10.5.9.2|    10.5.11.113|59587| 2293|  6|    0|3905120966|       1407623058137
    10.5.11.113|       10.5.9.2| 2293|59587|  6|    0| 150309616|       1407623058137
      10.5.12.2|    10.5.11.117|59699| 8888|  6|    0|3912451471|       1407623093677
    10.5.11.117|      10.5.12.2| 8888|59699|  6|    0| 582520324|       1407623093677
       10.5.3.2|    10.5.11.120|59746|  143|  6|    0|3915540661|       1407623114721
    10.5.11.120|       10.5.3.2|  143|59746|  6|    0|   9404760|       1407623114721
       10.5.2.2|       10.5.9.2|57432| 8888|  6|    0|3763882488|       1407523627665
       10.5.9.2|       10.5.2.2| 8888|57432|  6|    0| 582519576|       1407523627665
    10.5.14.107|    10.5.11.111|59014|47989|  6|    0|3867598385|       1407622961660
    10.5.11.111|    10.5.14.107|47989|59014|  6|    0|3145040834|       1407622961660
    10.5.14.107|    10.5.11.113|59503|   80|  6|    0|3899614474|       1407623040275
    10.5.11.113|    10.5.14.107|   80|59503|  6|    0|   5279029|       1407623040275
    10.5.14.107|    10.5.11.117|59541| 9001|  6|    0|3902097015|       1407623048722
    10.5.11.117|    10.5.14.107| 9001|59541|  6|    0| 589925835|       1407623048722
    10.5.14.107|    10.5.11.113|59578|  443|  6|    0|3904529633|       1407623055575
    10.5.11.113|    10.5.14.107|  443|59578|  6|    0|  29068768|       1407623055575
    10.5.14.107|    10.5.11.113|59587| 2293|  6|    0|3905121711|       1407623058137
    10.5.11.113|    10.5.14.107| 2293|59587|  6|    0| 150310297|       1407623058137
    10.5.14.107|    10.5.11.117|59699| 8888|  6|    0|3912452070|       1407623093677
    10.5.11.117|    10.5.14.107| 8888|59699|  6|    0| 582519917|       1407623093677
    10.5.14.107|    10.5.11.120|59746|  143|  6|    0|3915539932|       1407623114721
    10.5.11.120|    10.5.14.107|  143|59746|  6|    0|   9407537|       1407623114721
      10.5.14.2|       10.5.1.2|52646| 8888|  6|    0|3450228216|       1407526153262
       10.5.1.2|      10.5.14.2| 8888|52646|  6|    0| 582525670|       1407526153262
```

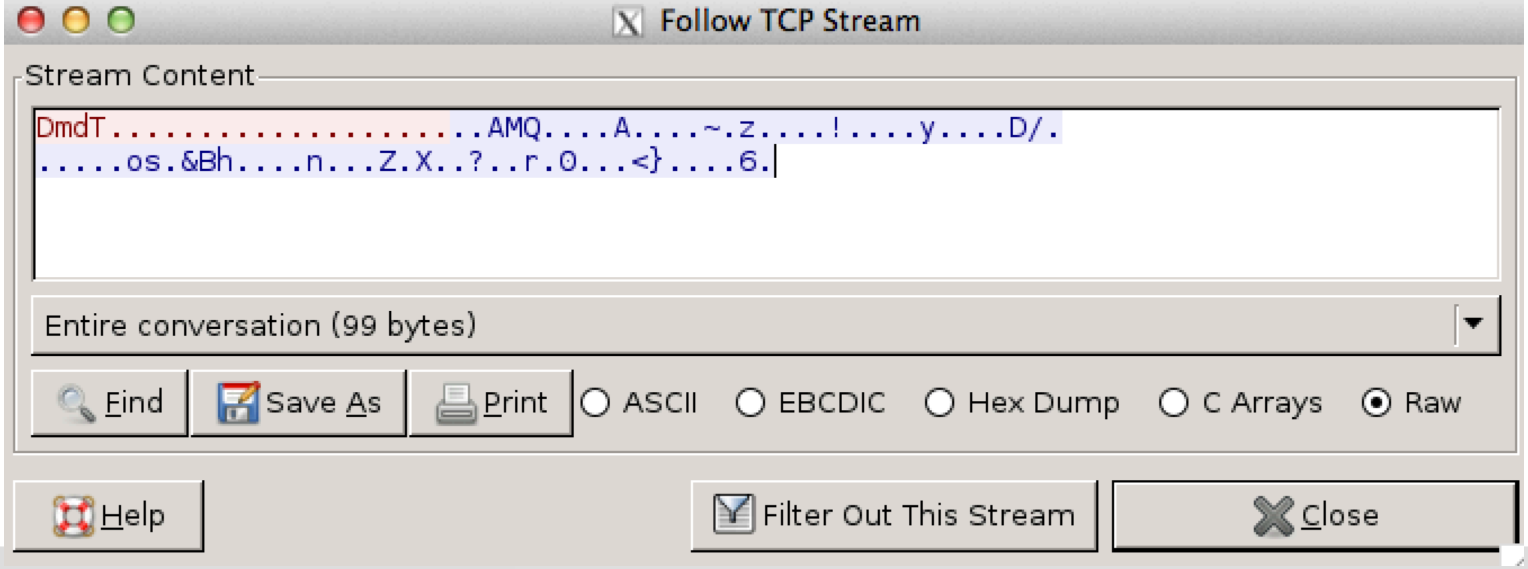
YafMeta2Pcap

Input:

- Large PCAP file or list of PCAP files
- PCAP meta file created by YAF
- Flow key hash and start time

Output

- PCAP file with desired flow



Follow TCP Stream

Stream Content

```
DmdT.....................AMQ....A....~.z....!....y....D/.
.....os.&Bh....n...Z.X..?..r.0...<}....6.
```

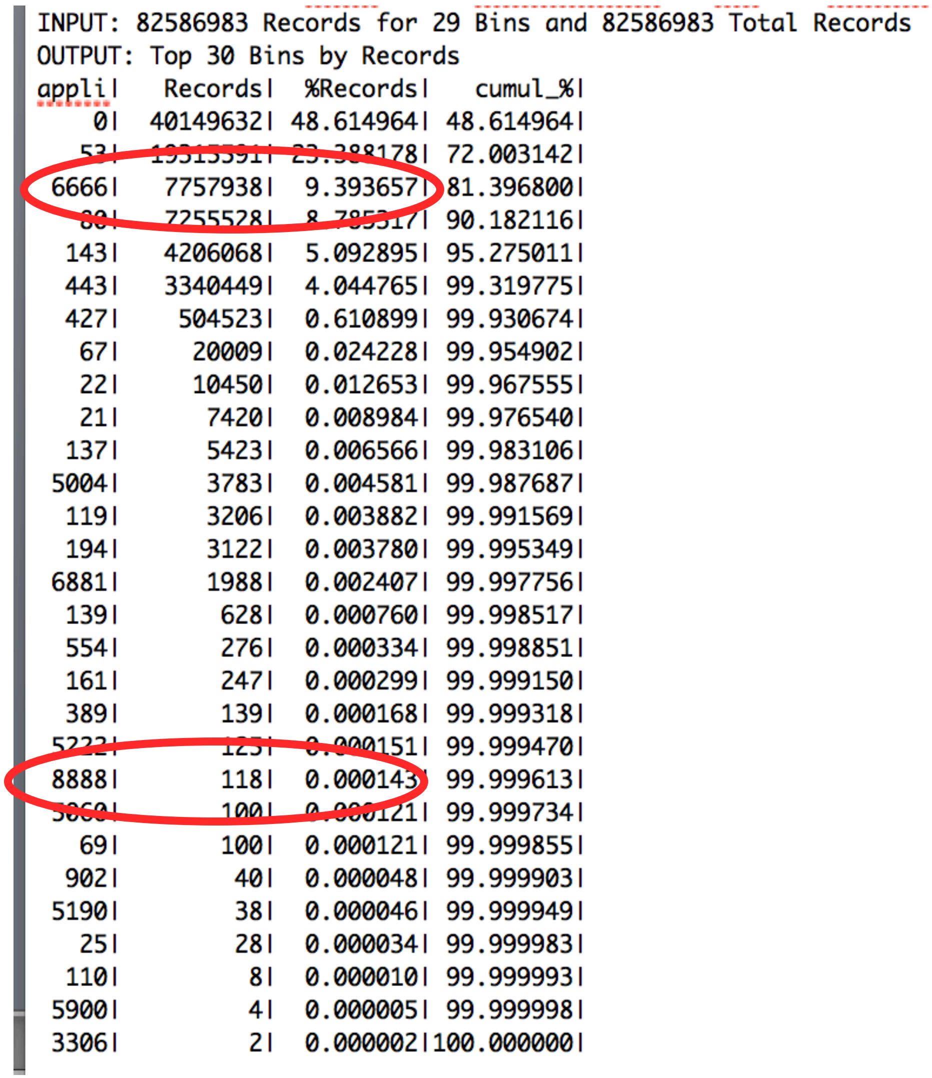
Entire conversation (99 bytes)

DEFCON Analysis

Used YAF signatures to determine other flows with “DmdT” and “eliza”

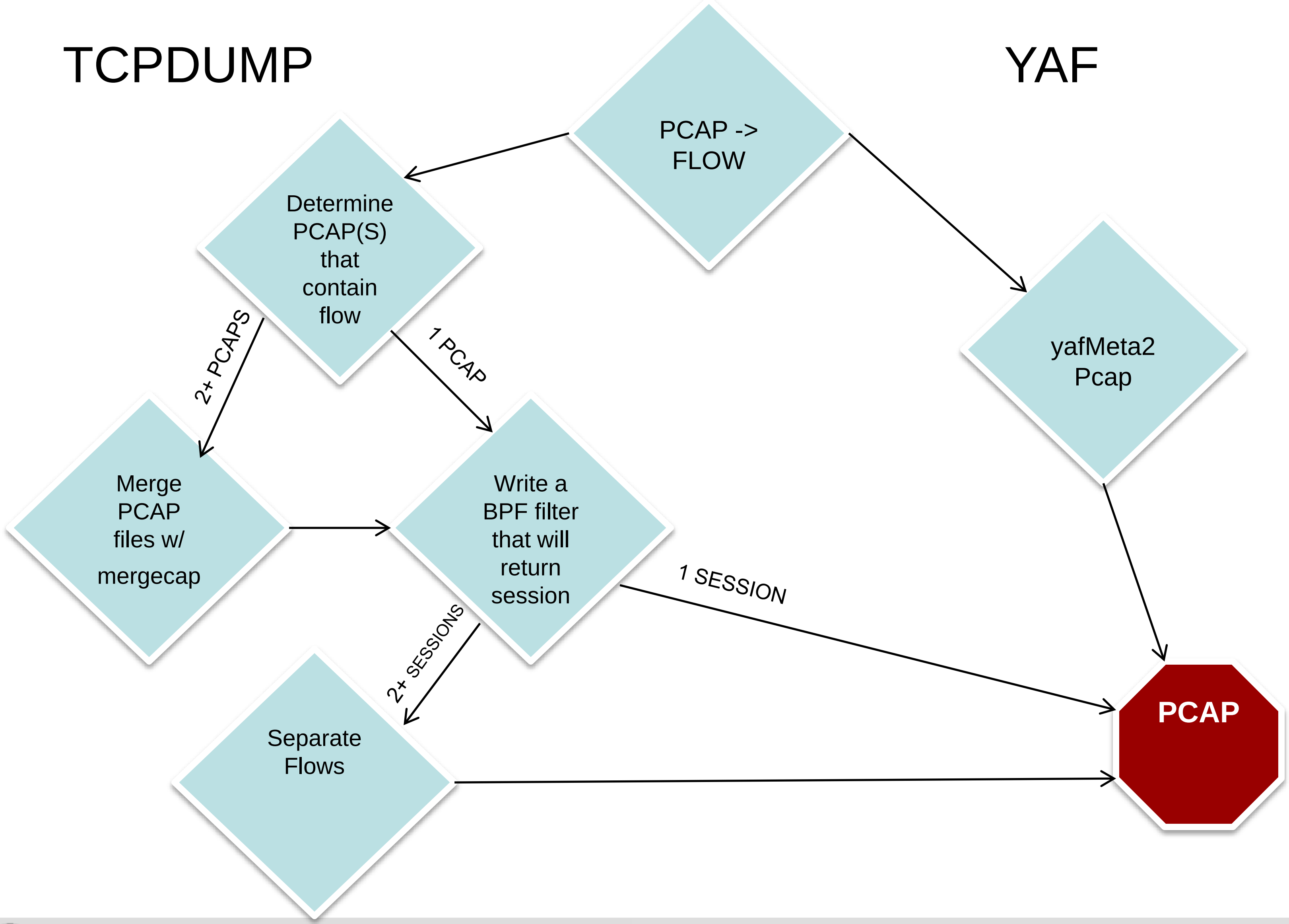
“eliza” was a text-based space economy simulator challenge at CTF

80% of DmdT traffic went to last place team.



```
INPUT: 82586983 Records for 29 Bins and 82586983 Total Records
OUTPUT: Top 30 Bins by Records
appli|   Records|  %Records|    cumul_%|
    0|  40149632| 48.614964|  48.614964|
   53|  19315391| 23.388178|  72.003142|
 6666|   7757938|  9.393657|  81.396800|
   80|   7255528|  8.785317|  90.182116|
  143|   4206068|  5.092895|  95.275011|
  443|   3340449|  4.044765|  99.319775|
  427|    504523|  0.610899|  99.930674|
   67|     20009|  0.024228|  99.954902|
   22|     10450|  0.012653|  99.967555|
   21|      7420|  0.008984|  99.976540|
  137|      5423|  0.006566|  99.983106|
 5004|      3783|  0.004581|  99.987687|
  119|      3206|  0.003882|  99.991569|
  194|      3122|  0.003780|  99.995349|
 6881|      1988|  0.002407|  99.997756|
  139|       628|  0.000760|  99.998517|
  554|       276|  0.000334|  99.998851|
  161|       247|  0.000299|  99.999150|
  389|       139|  0.000168|  99.999318|
 5222|       125|  0.000151|  99.999470|
 8888|       118|  0.000143|  99.999613|
 3060|       100|  0.000121|  99.999734|
   69|       100|  0.000121|  99.999855|
  902|        40|  0.000048|  99.999903|
 5190|        38|  0.000046|  99.999949|
   25|        28|  0.000034|  99.999983|
  110|         8|  0.000010|  99.999993|
 5900|         4|  0.000005|  99.999998|
 3306|         2|  0.000002| 100.000000|
```

Method Comparison


TCPDUMP
YAF
PCAP -> FLOW
Determine PCAP(S) that contain flow
2+ PCAPS
1 PCAP
Merge PCAP files w/ mergecap
Write a BPF filter that will return session
1 SESSION
2+ SESSIONS
Separate Flows
yafMeta2 Pcap
PCAP

Questions?

CERT NetSA tools website:

tools.netsa.cert.org

Contact:

ecoff@cert.org

netsa-tools-discuss@cert.org

netsa-help@cert.org

Presentation Abstract

Finding a needle in a PCAP

It can be difficult to find what we are looking for in a large PCAP repository, even when we know what to look for and where to look. When traffic captures start to enter multi-gigabyte sizes, the number of tools that can even begin processing these files is limited. SiLK and other flow analysis tools provide the tools for quickly narrowing down the search area but when ground truth is required, we are often back to square one when searching for a particular packet or flow in large traffic captures. This presentation will describe the available features in YAF for indexing large PCAP files with flow. We will provide relevant examples of common analysis techniques with various tools from the CERT NetSA Security Suite and how to perform complementary PCAP analysis with YAF. This presentation will also touch on deploying a tiered approach to network monitoring storage and ways to maximize storage without compromising network analysis.